Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life

Miguel Angel Olivero [a,*], Antonia Bertolino [b], Francisco José Domínguez-Mayo [c], María José Escalona [c], Ilaria Matteucci [d]

[a] *ISTI-CNR, Pisa, Italy, Web Engineering and Early Testing Research Group, Universidad de Sevilla, Seville, Spain*
[b] *ISTI-CNR, Pisa, Italy*
[c] *Computer Languages and Systems Department, Universidad de Sevilla, Seville, Spain*
[d] *IIT-CNR, Pisa, Italy*

Keywords:

Digital persona

Pluridentity

Portrayal

Privacy

Security

System of systems

ABSTRACT

The increasing use of the Internet for social purposes enriches the data available online about all of us and promotes the concept of the Digital Persona. Actually, most of us are represented online by more than one identity, what we define here as a *Pluridentity*. This trend brings increased risks: it is well known that the security of a Digital Persona can be exploited if its data and security are not effectively managed. In this paper, we focus specifically on a new type of digital attack that can be perpetrated by combining pieces of data belonging to one same Pluridentity in order to profile their target. Some victims can be so accurately depicted when looking at their Pluridentity that by using the gathered information attackers can execute very personalized social engineering attacks, or even bypass otherwise safe security mechanisms. We characterize these Pluridentity attacks as a security issue of a virtual System of Systems, whose constituent systems are the individual identities and the humans themselves. We present a strategy to identify vulnerabilities caused by overexposure due to the combination of data from the constituent identities of a Pluridentity. To this end we introduce the Digital Persona Portrayal Metamodel, and the related Digital Pluridentity Persona Portrayal Analysis process that supports the architecting of data from different identities: such model and process can be used to identify the vulnerabilities of a Pluridentity due to its exploitation as a System of Systems. The approach has been validated on the Pluridentities of seventeen candidates selected from a data leak, by retrieving the data of their Digital Personae, and matching them against the security mechanisms of their Pluridentities. After analyzing the results for some of the analyzed subjects we could detect several vulnerabilities.

1. Introduction

The concept of a *Digital Persona* has been introduced in the early ‘90 s [6] to denote the digital extension of an individual’s identity. Already more than two decades ago that work warned against the risks inherent in monitoring the “vast quantities of data ” maintained by “contemporary” business and government organizations [6]. Nowadays, the pervasive use of the Internet for ever-new social and business purposes has enriched and dramatically scaled up the data available about everyone on the network and hence boosted the concept of the Digital Persona.

The Internet is now commonly used to socialize by people all around the world. There exist social networks for nearly every imaginable topic. People communicate their interests and activities pushed by the human need of sharing what they like or do not like. Relationships on social networks are made of trust, reputation, and reciprocity with other users.

On the other hand, this phenomenon causes Digital Personae to be continually at risk, as the Internet is also a source of new opportunities of attacks [13]. There is an extensive list of different digital attacks depending on the purpose of the attacker and the possibility to interact with the victim [1,16,45].

The data that people make available can be used to analyze their profiles and study their behavior to predict their next actions [3,31]. Thus, our data have become a golden opportunity for attackers to learn about us, detect the incautious one, and design personalized attacks. Attackers need to preventively identify their

[*] Corresponding author.
E-mail addresses: miguelangel.olivero@isti.cnr.it (M.A. Olivero), antonia.bertolino@isti.cnr.it (A. Bertolino), fjdominguez@us.es (F.J. Domínguez-Mayo), mjescalona@us.es (M.J. Escalona), ilaria.matteucci@iit.cnr.it (I. Matteucci).

.

potential victims, and social networks ease the identification of the vulnerable targets.

Profiling people is a recent trend in digital attacks [4]: it entails using pieces of data freely available on the Internet and combining them to depict a targeted person. Some people publicly outline their Digital Personae so accurately that attackers can easily execute very personalized social engineering attacks [45], or even bypass some security mechanisms only by using the gathered information. These profiling attacks may have several consequences [43].

In this study, we draw attention on vulnerabilities of our Digital Personality that can arise due to what we call a *Digital Persona Portrayal* (DPP): by this term we refer to the unforeseen matching and combination of data sources corresponding to more identities we yield in different social contexts (i.e., a *Pluridentity*), altogether resulting in information overexposure that we may overlook.

These emerging vulnerabilities only exist because of the specific combination of several identities. To handle them we apply a System of Systems (SoS) [9,25] approach: we consider each identity as a constituent system, and the Pluridentity as the SoS. In a SoS, despite each system being secure enough on their own, the SoS security may be compromised by combining the available data from the constituent systems. Thus, the SoS vulnerabilities are only existing due to an Emergent Behavior [29] arising from a configuration combining the constituent systems.

We propose an original strategy for the assessment of vulnerabilities due to DPP. To this end, we first introduce models to structure and relate the data of pluridentities of the Digital Persona. Then we show how these models can be analyzed to identify potential DPP vulnerabilities.

The models, methods and techniques developed in our approach have been evaluated on seventeen subjects selected from a data leak from an online survey panel. For these 17 people, who all possessed more digital identities, we "portrayed" their Digital Personae, by retrieving and combining the data they exposed in differing contexts. In this evaluation, we took into account the security of those systems in which an identity of the Digital Persona was found, to determine the impact of potential attacks. After analyzing the results and matching the information about the identities of the Digital Personae, some vulnerabilities were detected.

1.1. Motivation

In information technology, the concept of a System of Systems (SoS) [9] has been introduced to denote a virtual distributed and composite architecture whose outcomes are achieved as the combination of the partial results from its constituent systems. In a SoS, the constituent systems keep their autonomy and in some cases they might even not be aware of the global mission to which they may be contributing: they just offer their service that, when combined one with another, allows for achieving some global goals that could not be reached by the individual systems alone.

Today, System of Systems and the System of Systems Engineering (SoSE) are seen as an opportunity for the systems engineering community to define complex systems [27].

We propose here a novel perspective in dealing with digital identities, i.e., that *users having more accounts on different systems can be understood as a SoS, whose constituent systems are the individual user identities.*

From the perspective of a SoS in the Digital Persona context, we look for attack vectors, paths or means that could enable an attacker to exploit the vulnerabilities in the SoS. The collaborative results produced after combining such systems in a SoS are named an Emergent Behavior. Such Emergent Behaviors can include expected results as well as unexpected results, as potential attack vectors that only exist for a specific combination of constituent systems.

Complex attacks that use data from various sources to create a profile of the people are named *doxxing*. People that are doxed can find their personal information published on the Internet, including postal address, national identity numbers or phone numbers, against their will. Attackers may collect this information from a single or many sources, and this information can be later used to make decisions about how to attack or harass the victim.

In this study, by using a SoS perspective, we study a specific type of doxxing attack, in which the gathered information about a persona, from different systems, is not directly used against the people, but to exploit the security of the identities of their Digital Persona.

This is a real problem with documented cases as the one that happened to Mat Honan.[1] Honan is a journalist who was victim of an attacker that gathered information available on various systems he used. The attacker combined information from one system after another until he could exploit the security on the systems where Mr. Honan had an identity. Eventually, the attacker impersonated Mr. Honan and deleted his entire digital existence. Similar problems have been identified in previous works [38] in the Systems of Systems context.

In this paper we introduce an approach based on related studies [22,30,33,52] to assess the security of the Digital Persona by considering the Digital Persona as a Virtual SoS in systematic way. This approach has been designed to support data management and verifying the security of Digital Personae as Systems of Systems, as part of the TeSSoS [39] approach.

To this end, three research questions have been defined:

- (RQ1) *What data items can be publicly found on the Internet about the users?*
- (RQ2) *What information can be generated when combining data from different sources?*
- (RQ3) *Could the overexposure become a vulnerability for the digital identities' security?*

To answer these questions, we contextualize the problem, and assess the SoS security by analyzing how the combination of the data coming from different digital identities can affect the security of the Pluridentity.

The vulnerabilities found when analyzing the identities that form a Pluridentity are understood as a vulnerability that emerges only from the combination of the data from several systems to exploit the security of another. In [46] the term vulnerability has been defined as "*A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy*". In this meaning, analyzing how identities are combined in a Pluridentity we can find vulnerabilities in the System of System design (the Pluridentity) each time it is possible to use the own SoS resources (each identity) to violate the SoS security policy.

1.2. Ethical considerations

The data used for validation in this study (Section 4) were obtained from a publicly available URL containing information that allowed identifying and profiling people. After noticing this fact, the website manager was notified to help them solve this problem. Consequently, they removed the data from the public web.

Our aim was not to use these data for any commercial or harming purpose, but as a real scenario to validate the presented approach, without using synthetic data. Thus, we performed the

[1] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

study without notifying the involved persons, because their informed consent or voluntary participation would have been a potential threat to validity. Notwithstanding this study has been conducted with the highest carefulness, and it should and must not entail and does not entail any harm for the analyzed subjects. This is enhanced by using in the paper a pseudonymized version of subjects' data. In this regard, instead of storing people real information, we used fictitious characters to represent each candidate. The activity has been carried out in compliance with Reg. EU 2016/679. More precisely, this study has followed the code of conduct and professional practice specific for the processing of personal data for statistical and scientific purposes, pursuant to article 20 (4) of Italian Decree 2018/101.

The data handled during this study has been manipulated according to the following principles:

(i) Publishing. The only purpose of using this data is academic and to provide value to the research.
(ii) Do not exploit. The data cannot be used to contact the people that these data refers to at any way.
(iii) Impermanence. The data can only be stored during the time this study is developed and published. After the reviewing process is completed and the work is published every trace of pluridentity used in this study has been removed.
(iv) Do no harm. The usage of this data cannot compromise the security of the subjects at any way.
(v) Anonymity. The data analyzed from the people shall be anonymized in such a way that it cannot be used to identify who this data refers to.
(vi) Confidentiality. The data cannot be shared, copied, printed, or distributed. The data cannot be accessed by any other people than the paper coauthors.

1.3. Roadmap

The remainder of this paper is structured as follows: Some patterns regarding Digital Persona overexposure and related works are mentioned in Section 2. Section 3 describes the methods, introduces the definitions, and shows the models. Section 4 provides the validation results from application of the described method. Finally, Section 5 outlines the conclusions.

2. Background and related work

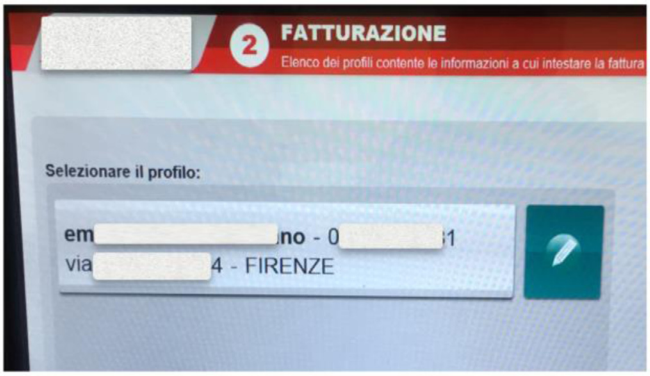
2.1. Background

The means of how systems acting as data sources can be reached by an attacker, the information that can be inferred from the data, and the value of this information concur to determine how secure a Digital Persona is.

Data items that can be found freely on the Internet might be part of the passwords or used to answer the security questions posed in the recovery passwords procedures. Among the typical security questions to recover the access when a password has been forgotten we can find: "When were you born?", "What is the name of your pet?" or "What is your favorite holiday destination?". These questions might however be easy to guess by a third party for subjects having a highly active social activity [43].

Patterns can be identified that enable a third party to reach some of this information by combining data and deduction. Looking at a social network profile, it is possible to read the name of the person and a picture, which gives an idea of the sex, age, and ethnicity.

This is not a lot of data, nevertheless it is enough to be identified, and allow personalized attacks aiming to harm or to retrieve further data as eWhoring [23].


[redacted] 2 FATTURAZIONE
Elenco dei profili contente le informazioni a cui intestare la fattura

Selezionare il profilo:

em[redacted]no - 0[redacted]1
via[redacted]4 - FIRENZE

Fig. 1. Self-service stand.

For instance, date of birth might be reached by using the following pattern. Day and month of birth can be obtained in any social networks by reading wishes and congratulation messages sent by other users. On the other hand, the year of birth can be derived from LinkedIn, based on which year did a cycle of studies begin.

Moreover, sloppy users posting photos of their pets in social networks may reveal sensitive data regarding their security questions.

Not only security questions are compromised, but also non-digital information can be used to exploit the human factor. Attackers could retrieve data by means of third people by using victim's personal information in a phone call, which could lead them to retrieve further data.

In a test case made by the authors to check the availability of information of people on third-parties' systems, we used a self-service stand that offers the possibility to print receipts after a purchase. This system offers a publicly available search feature, on which by typing a VAT number it retrieves the name, VAT number, and full postal address of the person as shown in Fig. 1, a photography of the screen of the stand. In this way, a client does not need to type all this data every time they want to print a bill. Notwithstanding, we were able to reach the billing data of another person by only using the VAT number we found in a visit card.

Combining the information of the visit card, and the information given by the search feature of the self-service stand, we were able to reach a new data: the home postal address. This could enable us using this information, for instance, in phishing attacks that simulate packages deliveries.

A well-organized pattern may allow an attacker to reach sensitive data of people and using this data to execute precise and targeted attacks. However, using these patterns in good faith may become a tool for self-analysis that allows an early detection of vulnerabilities in a DP.

It is worth noting that the combination of the available information from several systems is however not new. This strategy is based in the use of OSINT (Open Source INTelligence) which allows to gather extra information by using shared knowledge. OSINT applicability includes getting the geolocation through a picture. Despite a picture may not have the location in their metadata, OSINT makes it possible to know where a photo was taken just by analyzing the environment and related data [21].

2.2. Related work

Finding sources to retrieve people's data has been analyzed many times and by applying diverse strategies. There are some recurrent patterns for retrieving the data of a Digital Persona, being social networks the most common data sources. This motivated several authors to conduct their research in this domain.

Studying privacy problems, a study was conducted to determine how traceable is a username among different systems on the Internet [41]. This research line was continued by Malhotra et al. [30]. In their work the authors focused on applying techniques to measure the similarity of user profiles on different social networks. In the same year, Creese et al. [8] published a work in which they show how combining data coming from diverse sources may provide additional data and consolidate or disprove pieces of information. More reliable information could be devised looking for personal identifiers from a person, which could be obtained by looking for school grants announcements, or by their public information if they are freelancers [22]. Additional data that freelancers may also provide is their postal address when billing, which reduces to a single place the location of the person. All this information generates useful knowledge about a person that can be potentially used to exploit knowledge-based security on their systems [19].

The combination of data was later studied by Minkus et al. [33]. They worked in an experiment where they combined what people published on Facebook with data available in other sources. As a result, they were able to associate information from a data source to another to build a more precise profile of those people.

A more recent study describes a work where the authors used not only publicly available information, but also people behavior [52].

Recently, with the rise of wearables, in 2017 a study was conducted in which the authors analyzed how wearables may also constitute a rich source of personal data [2].

In Europe, to protect the user's data privacy, the GDPR (General Data Protection Regulation) [15] in Art. 15 deals with the right of access by the data subject. People have the right to know about how their personal data are being processed from the data hosting server, as well as the right to access their personal data and some specific details. To help in the use of their rights, some online services such as MDR (My Data Request) [32] help users in requesting their personal details to web system owners. These laws and services are useful for users to handle their personal information. However, ineffective mechanisms of authentication would allow an attacker to impersonate a victim and request their personal data through GDPR to obtain every information from this person. A recent study has confirmed such weakness in the human factor [11]. In this study the targeted people are not the only affected victims. In some cases, due to a human error, the data of third people are also leaked. This shows how the application of GDPR may become a two-edged sword when not using a proper requestor's identification. People might need to understand how exposed are their pluridentities because their overexposure is affecting how people are identified when accessing the data protected by the GDPR.

On the other hand, there are some legitimate services available for people who want to know if their identities have been recognized in any data leak or breach. These services are handy to discover if it is required to change the credentials of any identity in any place on the Internet. One of these tools that could be used to discover what other services do a DP use is HIBP (haveibeenpwned.com) [20]. Other services that could be used for analyzing the identities are SpiderFoot [47] and HPI-ILC (Hasso Plattner Institute Identity Leak Checker) [24].

SpiderFoot is a semi-automated reconnaissance tool that executes queries on different open data sources and retrieves matches for the input queries. This tool looks for identities' connection through the queried sources and tries to discover any coincidence or connection among them, also revealing where an identity is being used.

HPI-ILC is a simpler tool that allows querying by email address. It provides related personal data as telephone number, date of birth or postal address that has been made public on the Internet through data leaks. The advantage of this service, in contrast to HIBP, is that HPI-ILC allows one to know what other data could be made public in the leak. Additionally, this service protects the anonymity of the person, sending the report directly to the queried email address, avoiding data disclosure to curious people.

In the worst-case scenario, it is even probable to find some cases of records stored on third party systems as Pastebin.com, on which hackers publish the data leaks they get. Unfortunately, attackers may take advantage of the use of these data against their victims.

2.3. Comparison with related work

Several techniques for executing data gathering have been described, but they do not offer an explicit structure for handling the data. To the best of our knowledge, despite there exist tools and strategies for retrieving and analyzing public available data, there are no mechanisms to analyze or understand the impact of the overexposure on the Pluridentity as a System of Systems.

The concept of pluridentity that we apply to define a cluster of identities that represent a single person is like the one proposed in [22]. They introduced the concept of *super identities* as a set of individual elements from some identities. In contrast, this study has been founded in the use of a novel perspective, which is considering each participating data source as a constituent system in a System of Systems. The main difference is that in our approach we are not creating a new *super identity but* are putting together all the identities as constituent systems under the SoS prism. The vulnerabilities that emerge when combining the resources of constituent systems are thus SoS *emergent behaviors* that descend from a flaw in its design.

Previous works highlight the risk of having public data and how the data might be used against the people. These works, however, do not provide a clear example on how vulnerable the people are. The validation study conducted in this study by using the described method has detected security vulnerabilities caused by an overexposure that only exist when combining certain identities.

In summary, in this study we extend previous research on data gathering to propose the *Digital Pluridentity Persona Portrayal Analysis* method that standardize data gathering and security analysis, and the *Digital Persona Knowledge Model* and the *Relational Security Model*, which structure and analyze the gathered data.

A regulated procedure favors the creation of a metric to seize the exposition of a person. This approach can be systemized and partially automated, which may help people in self-analyzing their pluridentity configuration by themselves to detect security violations.

3. DP3A

A method named Digital Pluridentity Persona Portrayal Analysis (DP3A) has been designed to analyze if the available information about the identities could threaten the security of the Digital Persona. This method has been structured in two cyclic phases. The first phase is based on data gathering: i.e. collecting information from different sources and elaborating a profiling of the Digital Persona. Then, data are combined and used to create information about the identities that improves the knowledge about the Digital Persona (DP). The second phase challenges the security of the systems being used by the DP by using the generated information and knowledge.

3.1. Definitions

Some key terms need to be defined before describing the DP3A method. Some of the definitions exposed in this study are an extension of the definitions already given in previous works [7,12,48].

1. An *identity* is the virtual representation of an entity (e.g., your email account). An identity is associated with an entity through an identifier.
2. An *identifier* is a data-item whose purpose is to uniquely distinguish an entity given a context (e.g., your email address).
3. A *data-item* is a piece of data that belongs to an entity or identity (e.g., your surname).
4. An *identity provider* is a system that is able to generate identities that can be used in several systems (e.g., Gmail).
5. The *pluridentity* is a condition that refers to an entity, which is represented by more than one identity (e.g., your email account and your Instagram account).
6. A *user* is an entity that wants to access some system resources, generally by using an identity (e.g., you).
7. A *record* or *Data Record* is a set of data-items stored in one or more systems referring to a particular entity, identity, or pluridentity (e.g., your photos in Instagram).
8. A *Digital Persona* is a record that is rich enough in data-items to provide an adequate image of the represented entity or identity (e.g., your activity in social accounts or the emails you send).
9. A *portrayal* is the result of depicting a Digital Persona, by having a trace of each data-item conforming the record (e.g., a document summarizing the records belonging to your Digital Persona).

Considering these definitions, the first phase of DP3A is named *Digital Persona Portrayal*: it aims to describe the data gathered from different identities and give them a meaning. Then, the *Digital Persona Security Analysis* seeks to use previous gathered data to exploit the security of the systems being used by the Digital Persona.

In the following sections, these two phases are described.

3.2. Digital pluridentity persona portrayal

The Digital Persona Portrayal (DPP) is inspired by the Information Gathering phase defined by Mouton et al. [35], based in the social engineering attack cycle described by Mitnick and Simon [34]. Mouton et al. defined in their work a social engineering attack framework. Six phases were described that compose the identified activities that an attacker would do. After doing a “Target identification”, the authors describe the Information Gathering phase with three iterative activities: (i) identify sources, (ii) gather information from sources, (iii) assess gathered information.

During the DPP, sources are identified, information gathered and assessed, in essence a DP is portrayed. Portraying a DP consists of analyzing each identity that composes the pluridentity of the Digital Persona. In this analysis of the Digital Persona, data items are gathered, and the security requirements are described for each system on which the identities are being used.

A model has been designed to organize and combine the gathered data coming from each system. The model has been named the *Digital Persona Portrayal Metamodel* and is an extension of the Class Metamodel of UML [40].

The next section describes the activities that portray a DP by using the Digital Persona Portrayal Metamodel, which will be used later during the Digital Persona Security Analysis.

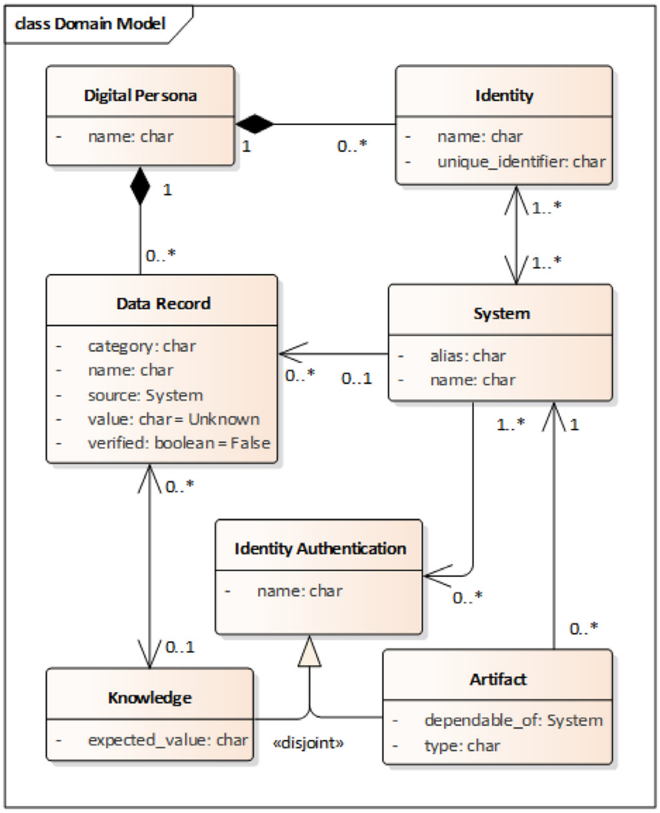


Fig. 2. Digital Persona Portrayal Metamodel.

3.2.1. Digital persona portrayal metamodel

The Digital Persona Portrayal Metamodel (DPPM) is shown in Fig. 2. It is used to structure the Data Records (DR) from a DP. This model includes seven classes:

(1) The Digital Persona (DP), in the top left corner, is composed of a set of Identities and Records. A DP is a class that represents the entity whose identities' security is being analyzed. The DP is identified by a name and may have two associated elements: the identities and the records.

(2) Identities, in the top right corner, are associated with one or more systems. The identities can be distinguished by email address, phone number, biometric data, etcetera, being email the most common online identifier for ordinary consumers [17,36,51].

(3) Systems, in the mid-right, that share the same identity are working under the same context. A system can be accessed through different identities belonging to the same DP. Systems may contain Records about the DP. Some records may include personal details that could lead the attacker to reach information about the physical identity of the victim. The system may also offer some security mechanism that, in the event of a successful authentication, offers privileged access to some data or actions. Identity Authentication is, however, not mandatory in every system. This is because there are systems providing classified data without requiring any identity authentication, as WHOIS, school grants or work website, among others. According to the authors of [26], such systems are a potential attack target for more than one DP.

(4) In the mid-left the Data Records coming from different systems may be combined by applying some knowledge about the DP to generate new data items that could enhance previous knowledge. Records may be used totally or partially

to exploit systems whose security is knowledge-based. DPs may provide records about third DPs, which may indirectly expose their identities.

(5) Identity authentication, in mid-bottom, is a security mechanism responsible for checking if the identity matches with the entity that is accessing these privileges. The authentication could be performed by using knowledge (i.e., what the persona shall know), or artifacts (i.e., what the persona shall own). The authentication can also be extended to biometrics (i.e., what the persona is), but in this study we considered only knowledge and artifacts.

(6) Knowledge, in the bottom left corner, is a subtype of identity authentication. Its strength resides on the use of a secret that third parties could not know. Typical Knowledge-based identity authentication uses passwords. This knowledge should not be found on the Records of the DP in any system. Nevertheless, in some cases there are systems that may provide data enough to generate this knowledge, which creates important vulnerabilities.

(7) Artifact, in the bottom right corner, is a subtype of identity authentication. The strength resides on the use of a system, which may be digital or analogical. Receiving an email in the inbox or a SMS in a mobile phone are examples of artifact-based identity authentication. These systems delegate the responsibility of the security on the security of another system that may even belong to another DP. Having access right to delegated system grants automatically access to every other system for which the former is responsible.

3.2.2. Portraying a digital pluridentity persona

The portrayal kicks off from some known information about the DP. Such initial data is taken as the starting point to look for any systems on which an identity of the DP could be exploited: thus, Internet searches are executed to find evidence of identities of this DP.

When an identity is detected, the system including it is evaluated twice. The first evaluation consists of considering the records provided by the systems in the context of the so-called *Digital Persona Knowledge Model (DPKM)*. On the other hand, the security features of the system are considered and modeled as a *Relational Security Model (RSM)* that focuses on the security among the systems and their dependencies.

DPKM and RSM are sub-models belonging to the DPPM model shown in Fig. 2. Each sub-model has a specific purpose, and their separation is illustrated in Fig. 3. The top part, containing Digital Persona, Identity, Data Record, and System, corresponds to the DPKM sub-model, which is used to organize the DR from a DP according to the identity and the system.

The bottom part, containing Data Record, System, Identity Authentication, Knowledge, and Artifact, corresponds to the RSM sub-model, whose purpose is to define the security mechanisms that protect the SoS.

Both sub-models enable an analysis of all records from all systems altogether, which can be used to identify a combination of data from different systems that exploits the SoS security.

Additionally, the Identity Authentication can be used as a criterion to constrain the search of records. Since the motivation for modeling the DP is to exploit the security on the SoS, data-items that are not relevant to exploit the security on the systems may not be considered. Fig. 4 illustrates how a system is understood as a combination of DR and security features, and how each part corresponds to DPKM or RSM, respectively.

During the portrayal process, the RSM is updated every time a new system of the DP is found. This update is required to refine the information needed to authenticate in knowledge-based systems. Then, the already queried systems in the DPKM are queried again to retrieve any data-item that may be related to the security of the new system. Systems are queried in the *First In First Out* order, looking for Data Records and for Identity Authentication. Each time some Data Record reveals that a new system in which the DP has an identity exists (e.g., a Facebook post reveals that a photo is available in an Instagram account), it is added to the queue and the process continues. The process ends when there are no pending systems to be analyzed. Fig. 6 describes this strategy.

When looking for identities of a DP two alternative methods can be considered. (1) A method in which the analyst avoids using data known in advance and limits the search on initial and found data. This blind search method would imitate how an attacker would initiate, i.e., without any detailed information about the victim. (2) In another method a full search is conducted by using every piece of knowledge about the DP. When using previous knowledge, a more complete model can be generated. This case would simulate a self-analysis.

The vulnerabilities found when analyzing the DPKM and RSM are understood as vulnerabilities that emerge by combining the data of certain systems to exploit the security of another. Thus, by using DPKM and RSM we can find vulnerabilities in the SoS design originating from the possibility to use the resources spread among the constituent systems to violate the SoS security.

3.2.2.1. Digital persona knowledge model. When searching the Internet for data about a DP, the DPKM sub-model is used for the analysis of information that provides knowledge about the DP.

DPKM focuses on the records in the DPPM and is used to categorize the data-items that could be used to exploit the security of the systems.

For better data handling, some predefined categories are proposed to organize the DRs according to their nature, including: Identifiers, Demographics, Location, Profession, Education, Economic, Social, Health, and Interests.

Those categories are based on those used to organize the census data in some countries.[2,3,4] Nevertheless, these categories can be adapted to best fit the analyzed context. Fig. 5 shows an anonymized DPKM from a laboratory study. In this figure, the Data Records are organized in categories as columns and the source system as rows. In this way every public DP is organized in a matrix that can be studied to detect vulnerabilities if these data are used as Identity Authentication in the RSM.

3.2.2.2. Relational security model. The Relational Security Model (RSM) focuses on the systems and their security. The goal of this sub-model is to organize the systems that are used by the same identity and point out which system is the identity provider. On the RSM, for each system the security is described according to its Knowledge or Artifact features. This model is used to guide the DPKM modeling, since the goal of DPKM is to collect enough data to generate information and knowledge that could be used to exploit the security described by the RSM. Fig. 7 shows an anonymized version of an RSM generated within a laboratory study. In this model each system is identified, as well as the responsible one, i.e. Identity Provider. For each found system the used security mechanisms are enumerated. Systems are organized according to the Identity being used in the systems. A system may appear more than once when a Digital Pluridentity Persona uses the same system with different identities.

Regarding the artifact-based security, by studying the dependencies among systems specified in the RSM, a dependency hierar-

[2] https://www.census.gov/acs/www/data/data-tables-and-tools/data-profiles/2017/

[3] https://www.ine.es/welcome.shtml

[4] https://ec.europa.eu/eurostat/web/ess/

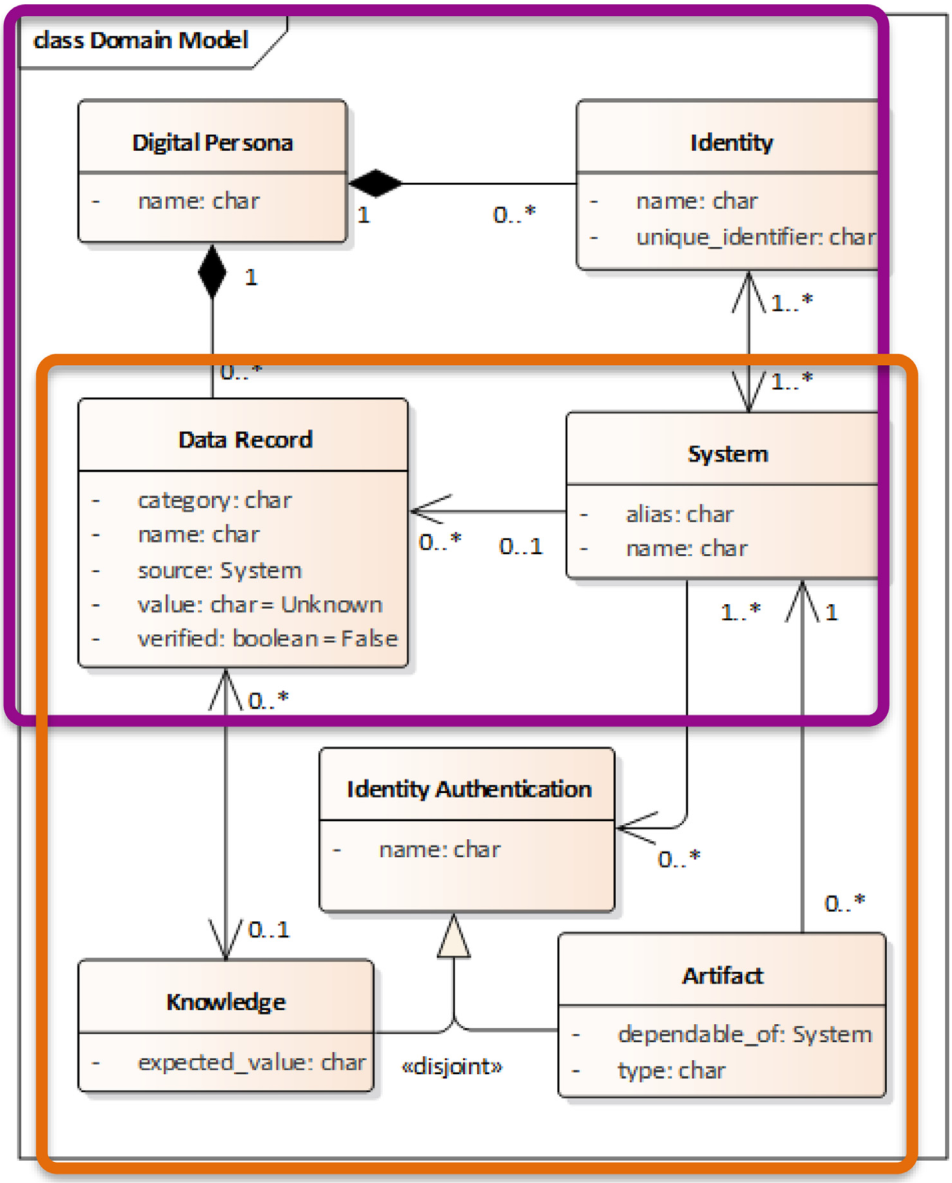


Fig. 3. DPKM and RSM.

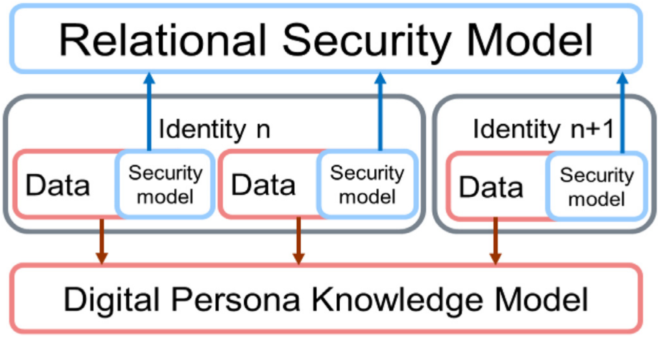


Fig. 4. Data and security models dichotomy.

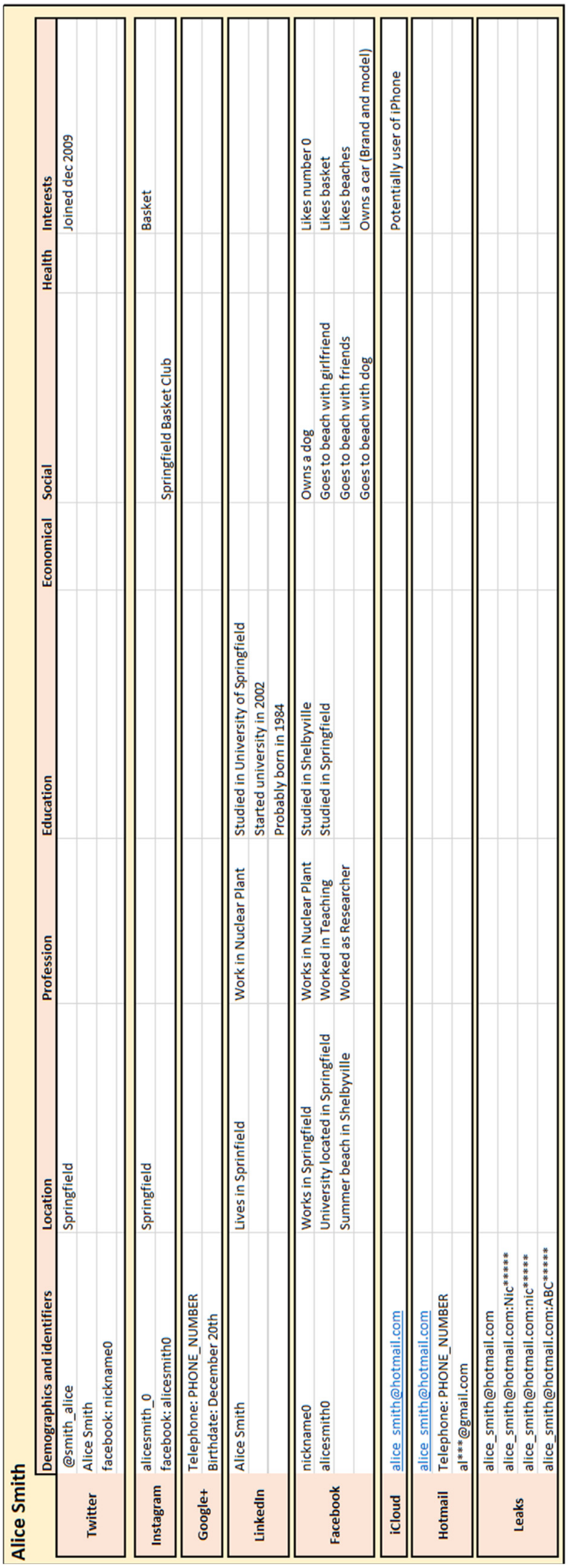
chy can be outlined. This chain of systems allows us to understand which systems have a higher responsibility, and thus should yield stronger security mechanisms.

The dependencies found in the RSM of Fig. 7 have been described as a Use Case model in Fig. 8, taking as use cases the systems depending on other ones.

3.3. Digital persona security analysis

Once the DPPM has been completed, through a combination of a DPKM and an RSM, further data can be inferred that help to discover attack vectors.

Potential attack vectors can be identified through analyzing already existing systems as record sources. For instance, as said, a set of congratulation messages on a social profile on a particular day, could disclose the day and month of birth. On the other hand, the year of birth could be extracted by analyzing other factors, as for instance when the persona started the high school or the university. In this way, any security question regarding the birth date can be answered, and thus systems using this information as knowledge-based security can be considered insecure [19,43].



Alice Smith

	Demographics and identifiers	Location	Profession	Education	Economical	Social	Health	Interests
Twitter	@smith_alice Alice Smith facebook: nickname0	Springfield						Joined dec 2009
Instagram	alicesmith_0 facebook: alicesmith0	Springfield				Springfield Basket Club		Basket
Google+	Telephone: PHONE_NUMBER Birthdate: December 20th							
LinkedIn	Alice Smith	Lives in Sprinfield	Work in Nuclear Plant	Studied in University of Springfield Started university in 2002 Probably born in 1984				
Facebook	nickname0 alicesmith0	Works in Springfield University located in Springfield Summer beach in Shelbyville	Works in Nuclear Plant Worked in Teaching Worked as Researcher	Studied in Shelbyville Studied in Springfield		Owns a dog Goes to beach with girlfriend Goes to beach with friends Goes to beach with dog		Likes number 0 Likes basket Likes beaches Owns a car (Brand and model)
iCloud	alice_smith@hotmail.com							Potentially user of iPhone
Hotmail	alice_smith@hotmail.com Telephone: PHONE_NUMBER al***@gmail.com							
Leaks	alice_smith@hotmail.com alice_smith@hotmail.com:Nic***** alice_smith@hotmail.com:nic***** alice_smith@hotmail.com:ABC*****							

Fig. 5. Alice's DPKM.

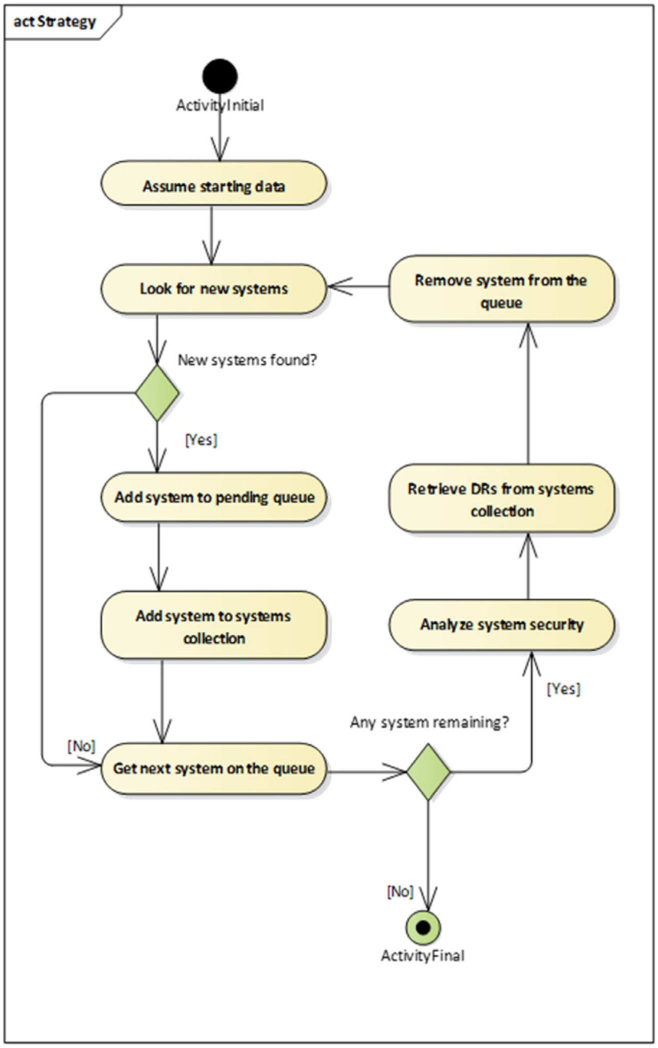


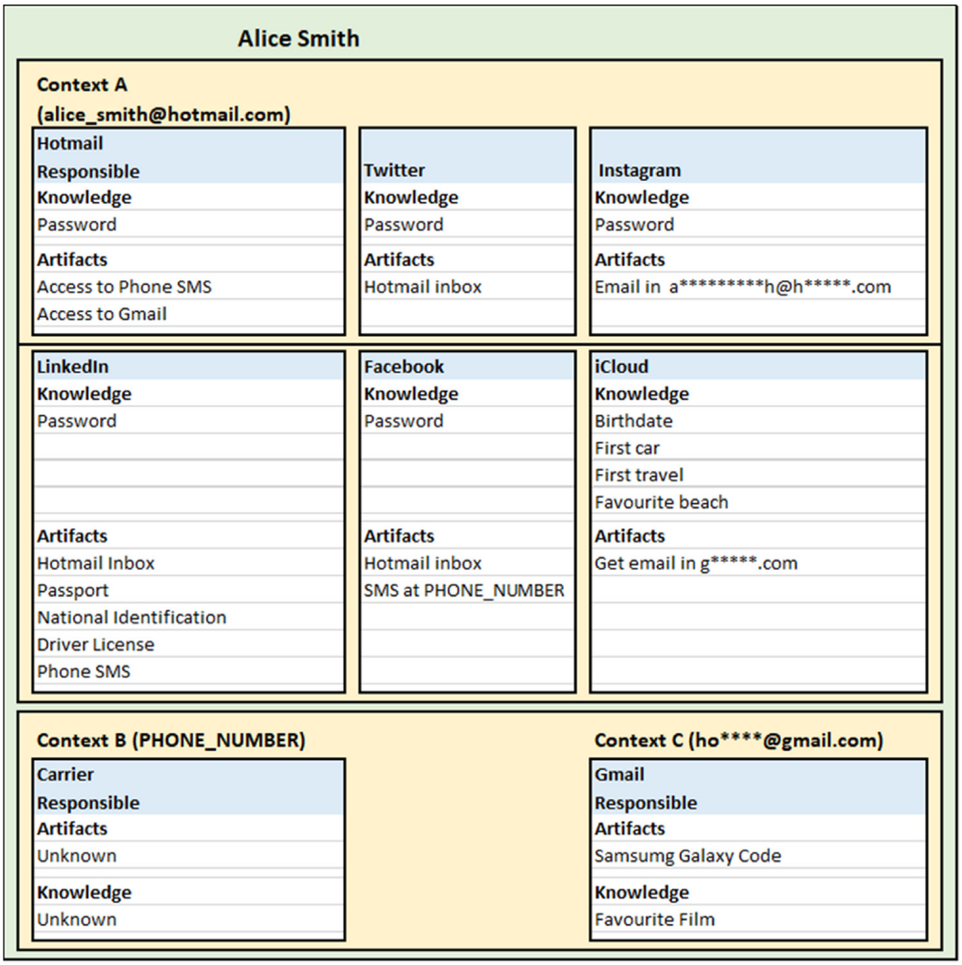
Fig. 6. DPPM strategy.

As Gross et al. refers in their work [18] some people do not care about the risks entailed in making their data records publicly available, and rather prefer to receive wide social feedback.

People may use best-kept secrets for their knowledge-based security. In this case, attackers could launch social engineering attacks to target these precise data. The more information the attacker can use, the more sophisticated the attack can be and thus the more difficult it will be to detect the attacks.

Defensive strategies may include removing information that expose sensible systems, identities, or records to an attacker. However, even suddenly hiding data may raise suspects that there is something valuable worthy hiding. This may have the secondary effect of making people curious about what data were there before, increasing the motivation to access them. This is known as the Streisand effect. An attacker that is collecting data when doxxing may overlook some details, however trying to hide them may highlight them as quite relevant, attracting more attention and producing the opposite effect.

The analysis of the DPPM could generate metrics of how much exposed the DP is according to how much information could be found. This metric could rate the security of the identities of a DP and establish if a DP is more vulnerable than others to receive attacks.



Alice Smith

Context A (alice_smith@hotmail.com)

Hotmail Responsible
Knowledge
Password
Artifacts
Access to Phone SMS
Access to Gmail

Twitter
Knowledge
Password
Artifacts
Hotmail inbox

Instagram
Knowledge
Password
Artifacts
Email in a*********h@h*****.com

LinkedIn
Knowledge
Password
Artifacts
Hotmail Inbox
Passport
National Identification
Driver License
Phone SMS

Facebook
Knowledge
Password
Artifacts
Hotmail inbox
SMS at PHONE_NUMBER

iCloud
Knowledge
Birthdate
First car
First travel
Favourite beach
Artifacts
Get email in g*****.com

Context B (PHONE_NUMBER)

Carrier Responsible
Artifacts
Unknown
Knowledge
Unknown

Context C (ho****@gmail.com)

Gmail Responsible
Artifacts
Samsumg Galaxy Code
Knowledge
Favourite Film

Fig. 7. Alice's RSM.

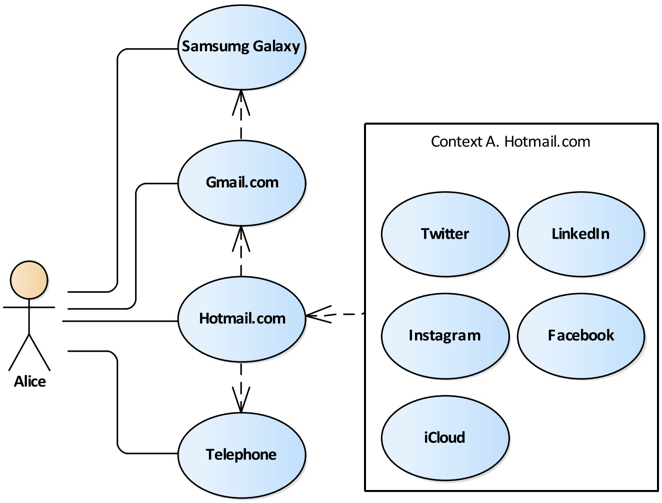


Fig. 8. Alice's systems and responsibilities.

4. Evaluation

The DP3A method was evaluated on 17 anonymized subjects to validate the performance of our approach in detecting vulnerabilities in the security of their pluridentities. This study began with email addresses as the only known data about each DP. The aim of this laboratory study was to collect as many data as possible of the candidates and evaluate if their security is or can be compromised (i.e., with reference to the two methods described in Section 3.2.2, we use the blind alternative). Due to ethical reasons, no actual attack or doxxing has been perpetrated, and no interaction was made with the candidates, neither with their systems or identities beyond that of documenting their security requirements or retrieving public data.

The evaluation has been structured in three stages:

(1) Setting up. The process followed to select the candidate DPs is decided;
(2) Execution. The data gathered for each DP are organized according to the DPPM;
(3) Data analysis. The last stage is to analyze the DPPM produced for each candidate to detect any security issues.

In the following we include a separate subsection for each stage and conclude the section by discussing the threats to validity.

4.1. Setting up the SoS

The validation of the DPPM model and the DP3A process has been conducted over a population of 5234 users made available from a data leak from an international online survey service.

The SpiderFoot HX tool [47] was used during its private beta phase to ease the analysis of the candidates, which is a prohibitive number for a manual analysis. This tool gathered data by querying a set of public APIs by username based on the email addresses. The purpose of using this tool is to automate the first scan of the

Table 1
Top 5 alternative Identity provider.

Top Identity provider	Users
hotmail.com	2372 (55,98%)
gmail.com	1271 (29,99%)
yahoo.es	133 (3,13%)
hotmail.es	120 (2,83%)
msn.com	51 (1,20%)

email addresses. Precisely, SpiderFoot HX allowed two batches of queries up to 300 different entries, which was split into 18 sets. 600 email addresses were being examined simultaneously. With durations from 2 h and 41 min to 6 h and 40 min, a total time of 19 h and 13 min, spread over three days, were needed to complete this automatic scanning process. The data regarding each email addresses batch was retrieved in a compressed *.csv type file of about 2Mb. The same file uncompressed reached 200Mb on average for 300 candidates.

Overall, according to SpiderFoot HX results, the whole set of candidates was using 510 unique systems, with a total of 33,174 connections among users and systems. 69,76% of the candidates are using from 2 up to 6 systems with the same identity. Among these, false positives may occur due to homonym identities, i.e., the same username may belong to different entities; or due to unusual behavior on the social profiles [37]. We handle such cases in the following manual analysis.

After a first analysis of the data leak used as source, 4237 valid email addresses were detected. The remaining 941 entries were phone numbers, names, or not well formatted email addresses. Notwithstanding, seeing that 4237 is a soaring number of people to manually apply the proposal, a criterion for selecting few cases is needed.

A script in Python was developed to automatically read the CSV file and extract relevant information. This script can be found in a public GitHub repository,[5] whereas due to the nature of the data in the csv files, those files cannot be published. The script revealed that many data records had been revealed in well-known data leaks (e.g., "*collection4g*", "*collection4eu*", "*collection4u*", "*onlinerspambot*", "*collection1*", "*exploit*"). We decided to omit such systems from our analysis (despite these data may generate a huge vulnerability for the DP), since such systems are not directly managed by the users. These leaks involved 1664 (38,76%) identities, which appeared in at least one leak. 61,23% of the leaks involved identities managed by Hotmail (1019 identities), the second most affected identity provider was Gmail with 29,63% of the leaks (493 identities). A total of 134 different digital identity providers among the analyzed ones were found. Despite the diversity, more than 93% of the population uses the same top 5 identity providers. The top five identity providers used by the users of the online survey system are shown in Table 1.

In general, the higher the number of social networks in which people appear, the more exposed they are. In fact, social networks are a useful source to extract data about someone and their friends or followers [19,52]. Hence, in this study we decided to select those users that were identified by the SpiderFoot engine in Facebook, Instagram, Twitter, and LinkedIn. From an analysis of SpiderFoot results, 17 people are using those social networks.

The DP3A process was applied to these 17 candidates, taken as representative of the average active user on the Internet for the purpose of this research. From here we continued the study manually with the most exposed candidates.

After collecting the data from the DP, the study continues with the usage of the DPKM to analyze the DP data records and the RSM to analyze the security on the systems.

4.2. Executing DP3A

For each selected candidate, we started the Portrayal to create models of their DP pluridentity. We instantiated a DPPM model for each candidate which allows us to analyze the data found and the security mechanisms being used in each system. The process started by analyzing the security mechanisms of the identity provider and looking for systems in which the needed knowledge might be used. As said, blind search strategy was applied and no contact with the people was established. This decision was motivated to prevent that, by noticing that their data are being analyzed, they might do some modifications and invalidate our study. People are increasingly aware about privacy and the risks of publicly available information, and their reaction could affect the results [5,28].

During the process, new identities appeared referencing the DP being studied. Each time a new system or identity was discovered, the data of already analyzed systems were considered again, trying to get enough data to exploit the security of the pluridentity. We analyzed each candidate one at a time, until no more data for a candidate could be retrieved.

We remark that this execution phase has been conducted only by using public data, without using any data leaks (beyond the original source of the used data) or exploiting any system for acquiring further information about the candidates, as declared in the ethical considerations. This limitation was constantly considered despite in some cases it would have been possible to retrieve data-items that could dramatically expose the security of the DP and its identities. Clearly, a true attacker would not employ a similar care, and thus the actual risks could be higher than the ones we assessed.

This laboratory study has been used to answer the research questions that lead this research (Section 1.1).

RQ1 stated: "*What data items can be publicly found on the Internet about the users?"*

Analyzing the data gathered on the DPPM, it was possible to determine: the physical location of 10 candidates (58%), the working position of 8 (47%), the interests of 6 of them (35%), and the education or training, as well as some economical details, of 3 candidates (17%). Pictures of some faces were also retrieved. Faces found were also used as a source of information to conduct a reverse image search and to provide additional information about the people [42]. A total of 8 faces were found and used, allowing facial identification of 47% of the candidates.

At the end of the analysis of the 17 candidates, a total of 40 different identities were revealed, having each candidate on average 2,35 identities. In total 82 systems were identified that allowed retrieving personal data from the email owners.

Having these data from the candidates, the data were combined to generate further data.

The results of applying the DP3M over the 17 candidates are summarized in Table 2. On this table, for each candidate and each category, a "Y" is placed if relevant data was found and could be exploited, a "N" if no relevant data was found, and a "P" if the data partially reveals any relevant information.

Subject #6 is the topmost exposed candidate, offering data enough for a full identification through their SoS configuration.

The detected causes that helped in gathering information from these systems have been:

–The candidates published their email address to be contacted and receive feedback.

[5] https://github.com/miguel-olivero/Spiderfoot-Analyzer

Table 2
Results of manual analysis on 17 candidates.

ID	Demographics & Identifier	Location	Prof	Education	Economical	Social	Health	Interests	Identity providers	Artifacts	Knowledge
1	3 identities, 8 systems Full name	Y	Y	Y	N	N	N	N	Gmail x1 Hotmail x1	Another inbox Phone number	Who invited you to Gmail?
2	3 identities, 4 systems Full name	N	N	N	N	N	N	N	Gmail x1 Hotmail x1	Another inbox Phone number	Dog name
3	2 identities, 3 systems Partial name	P	N	Y	N	N	N	N	Gmail x2	Another inbox	When was the Gmail account created?
4	2 identities, 4 systems Full name Partial birth date	Y	Y	Y	P	N	N	N	Hotmail x1 Work email x1	Another inbox	–
5	2 identities, 4 systems Full name Partial birth date	Y	Y	N	P	Y	N	Y	Telefonica x1 Gmail x1	Another inbox Phone number	National ID number Name Birth date
6	3 identities, 10 systems Full name Partial birth date	Y	Y	Y	Y	Y	N	Y	Gmail x2 Work email x1	Phone number Tablet Another inbox	Favorite superhero
7	3 identities, 3 systems	N	N	N	N	N	N	N	Hotmail x2 Gmail x1	Another inbox	How far do you want to reach today?
8	1 identity, 1 system	Y	Y	N	N	N	N	N	Work email	–	–
9	3 identities, 8 systems Full name	Y	Y	N	Y	N	N	Y	Gmail x2 Work email x1 Hotmail x1	Phone number Another inbox	First teacher name
10	3 identities, 4 systems Full name	N	N	N	N	N	N	Y	Gmail x2 Hotmail x1	Phone number Another inbox	Backup code Frequent flyer number
11	1 identity	N	N	N	N	N	N	N	IDENTITY NO LONGER EXISTING		
12	3 identities, 4 systems Partial name	Y	N	N	N	N	N	N	Gmail Hotmail x2	Phone number Phone device Another inbox	First teacher name
13	3 identities, 10 systems Full name Partial birth date	Y	Y	Y	Y	Y	N	Y	Hotmail Gmail Yahoo		–
14	2 identities, 3 systems Partial name	P	N	N	N	N	N	Y	Hotmail Gmail x2	Phone device Another inbox	First teacher name
15	1 identity, 7 systems Full name	Y	Y	N	N	N	N	P	Gmail	USB stick	–
16	2 identities, 5 systems Partial name	Y	N	N	N	N	N	N	Gmail Outlook	Phone number Phone device	Grandmother surname
17	3 identities, 3 systems	N	N	N	N	N	N	N	Hotmail x3	Another inbox	–
T	40 identities, 82 systems	10 Y 58%	8 Y 50%	5 Y 30%	3 Y 17%	3 Y 17%	–	6 Y 35%	–		

–The name of the candidate appears on the email address.
–The candidates use the same name in the email address and in social networks.
–The candidates use alternative identities as recovery methods, that are disclosed when "Forgot my password" is used.
–The email address appears in a leak disclosing the interests of the candidates.
–Their email address is published on personal websites or work websites, as GitHub.
–The candidates shared information about their own from a social network to another.
–The candidates use the same profile picture on several systems.
–The candidates are using one same username across different systems.
–The candidates have a relevant position in a company that is listed in public documents of the government.

Subjects #2, #7, #10, and #17, were the most hidden ones. It was not possible to get additional information about their identities.

Using an identity that does not provide information enough reduces the chances of an attacker reaching further data. This also helps in avoiding being tracked to other systems or other identities, which could improve the security of those DPs.

On the other hand, homonymous identities make tracking difficult. Using automated search to determine the usage of systems by email address was not a conclusive result since the same identifier was being used by different entities in different systems.

The reasons for having difficulties on gathering information about the candidates have been:

–Few data available to start the portrayal from the email address.
–No social network found.
–Private social networks.
–No longer existing domain address.
–No contact data available for private blog or domains.

During the analysis of each candidate, a DPPM model has been created as a combination of a DPKM and an RSM. The use of DPKM and RSM help us in answering RQ2: "*What information can be generated when combining data from diverse sources?*"

Precisely, DPKM helped in collecting all the information available and RSM guided the collection process by limiting the scope and focusing on the relevant data. Figs. 5 and 7 shows the DPKM and RSM models of an anonymized candidate we refer to as Alice. By matching the data gathered from the DPKM, and the identity authentications from the RSM we aim at detecting potential security vulnerabilities.

Considering her Pluridentity, Alice was providing data such as name, email address, year of birth, phone number, city, where she studied, what she studied, pets, and sports. These data can be used to send specific attacks to retrieve further data and thus making Alice and her SoS increasingly exposed.

Three identities were found for Alice's DP, and eight systems were associated with these identities. For each system, the security and the data were documented, which produced the RSM.

The RSM is studied to keep track of which systems could be exploited and which system depends on another. In Fig. 7 the systems from Alice are organized according to the identity being used. This makes it possible to determine a cascade vulnerability on systems that rely on the artifact security of other systems. The purpose of this analysis is to model Alice's Digital Pluridentity Persona as a SoS. From this model we can determine which is the most critical system that could compromise any other, and to identify sources of vulnerabilities. This model can also allow us to enumerate and prioritize the existing vulnerabilities in the SoS.

For example, we could realize that if Alice loses her phone or her tablet, as a consequence all her DIs are potentially compromised.

In fact, the systems found in this analysis were providing pieces of information about her that allowed us to reach an iCloud account created with a Gmail identity. The security on this system was critically compromised. Despite this system provided two-factor authentication, Alice had not activated it. Regarding knowledge-based security, iCloud provides recovery methods based on security questions. Those questions are birthdate, first car, favorite beach, and the destination of the first travel by plane. Some of these questions can be answered by the data published by Alice in social networks and others can be deducted by reasoning on the acquired knowledge.

In general, if an attacker gains access to one system of Alice's DP, this one could become a new source of personal data that could be used for malicious acts. This problem has been studied in other works as [43]. Potentially an attacker could hijack Alice's phone or tablet, discover her precise location, access documents and photos, among others, as happened in 2014 in "The Fappening".

The way pieces of data of distinct categories, often coming from different systems, were combined to find additional data or to generate new data is shown in Fig. 9. This data deduction is similar to the one already conducted by Creese et al. [8]. In their work the authors developed a matrix easing to understand what data could be inferred according to already published data.

When considering the social profiles as a System of Systems, this derived data does not belong to any single system, but instead belongs to the DP, since it has been generated from a merged result. By using the SoS prism, it can be considered as an Emergent Behavior [29]. The combination of the information on those systems produces a set of data that would not be reachable differently.

4.3. Analyzing SoS security

After gathering the data from each system of each candidate, the analysis of the DPKM and RSM allows us to study the available data and detect security issues among the different systems.

In this section the 17 candidates are evaluated as if they were Systems of Systems, on which their security is analyzed according to the ability of exploiting the SoS security by using the resources provided by the constituent systems.

Regarding the security on the systems of chosen subjects, 4 (23%) of them have delegated the security of their identities to an artifact, e.g. a USB stick, or another device with an authenticator software; 8 (47%) of them to receiving a SMS in their mobile phones; 13 (76%) are trusting on receiving a code via email using other identity; and 11 (64%) uses a security based on knowledge.

Considering the collected data, candidates #7, #11 and #17 are the best secured DIs since we could not get any other information that helped us in identifying the individual. No data was found for #2 either by using the techniques considered in this study. Nevertheless, we detected the DIs were used in some systems and an attacker in a real attack could use more aggressive strategies to enable further data retrieval.

Among the users that rely on knowledge-based security, the most exposed one is candidate #6, revealing full name, birth date, and relevant data from each category. This DP is using three identities, and a weak point was detected: one of the identities can be exploited by answering "favorite superhero". By knowing personal details of this candidate, an attacker could attempt to create a close relationship and retrieve this information.

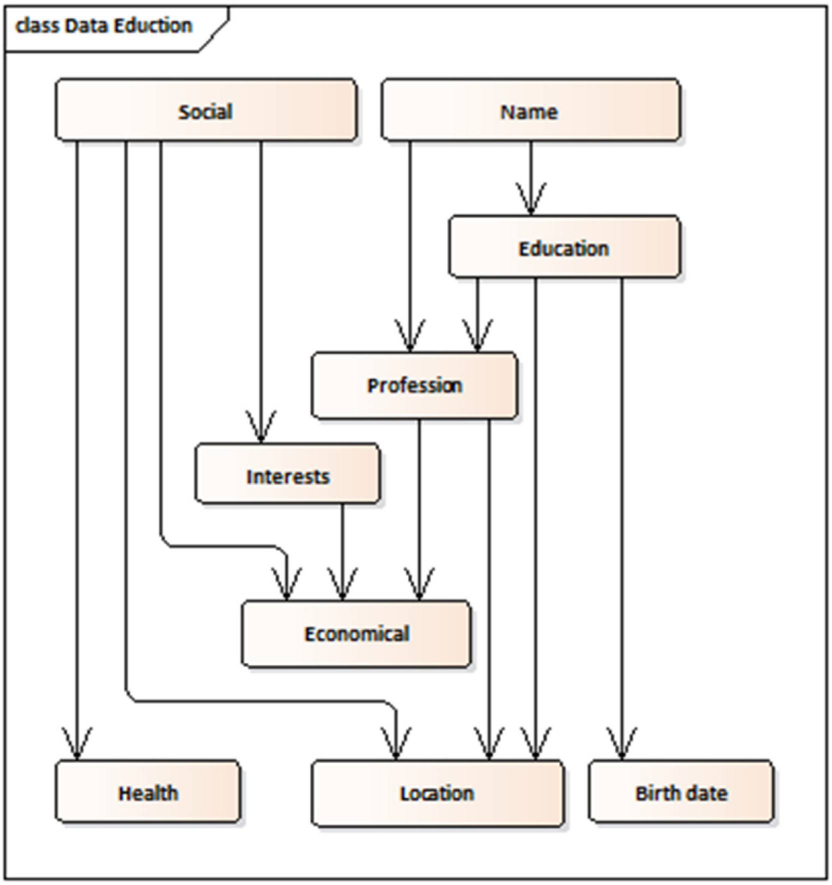


Fig. 9. Average personal data deduction.

Candidate #13 is as exposed as #6 but is considered more secure since the revealed data is not compromising the security of any identity. This consideration could change if a new identity comes into play using an exploitable knowledge-based security.

Hence RQ3 "*Could the overexposure become a vulnerability for the digital identities' security?*" can be answered considering both candidates. Overexposure of a DP can become a vulnerability for the digital identities if, among the systems being used by the DP, any of them is using a knowledge-based security that could be bypassed by using exposed data.

As said, knowledge-based security could be exploited by establishing contact with the victim. On the other hand, artifact-based security is not necessarily a safer choice. When the identity authentication is artifact-based, a security mechanism must be established to protect this new system. In this sense, unless there is a loop of artifact-based security systems, the security of the systems must eventually end in a knowledge-based secured system, or even worse, in an unsecured system.

Knowledge required to exploit the security of these people include answering to: how invited to Gmail, dog name, first phone number, full name and phone and birthdate, favorite superhero, daily top goal, first teacher name, frequent flyer number, eight-digit backup code, when Google account was created, and grandmother surname.

The most used artifact-based security is receiving an email in an alternative inbox. Second topmost used mechanism for recovery access to a system is based on Two Factor Authentication (2FA). 2FA can be managed by using exclusive apps or by receiving an SMS that provides a code to be typed by the user. However, smartphones can be stolen, and in some cases, people do not have a proper protection mechanism. In other instances, SMS can be obtained since these messages are sent without an encryption method. An even more complex way to break 2FA is SIM swapping,[6] in which attackers duplicate a SIM card allowing them to receive every SMS used in any 2FA protocol [44].

This method and report might be executed for self-analysis to analyze the weakest points in the DP.

4.3.1. Threats to validity

To understand the context and limitations of this study we enumerate the internal and external factors that could impact the results.

Internal validity concerns whether the outcome of the study could descend from other factors than the information overexposure in SoS. Internal validity may be threatened by the selection of subjects, and the effects of the study on user's privacy. The chosen subjects were active users from a Spanish online polling panel. Among them we could recognize people of different gender and age. Subjects also had different occupations: students, public employees, freelancers, and professors. People using this panel were from countries all around the world such as Argentina, France, Italy, Mexico, Spain, or the United Kingdom. Notwithstanding the culture of the people and their education could impact the results of this study: perhaps different subjects might be more cautious in exposing reserved information. To mitigate this risk, we would need to conduct more studies on different sets of users from other communities. However, any such study may impact user's privacy thus we preferred not to handle further sensitive data.

[6] https://www.bbc.com/news/business-46047714

Concerning the study effects, a threat to validity may derive from our extreme care in avoiding any impact on users. By conducting more aggressive, careless testing (as perhaps a true attacker would do) could have produced more data, but also affect the study outcome. Candidates could eventually get notice that their data is being used or queried, and thus take countermeasures that would block the analysis. In any direction, there are involved threats: we opted for the milder action to safeguard the candidate's privacy.

On the other hand, *external validity* (i.e., whether and to what extent the outcomes can be generalized beyond the study subjects) is threatened by the setting and the timeliness. As a whole candidates had an active digital participation according to our findings, however we cannot guarantee that this phenomenon occurs if replicating this study with a different population. Systems and security in digital life are quite different from candidate to candidate. Again, to mitigate this risk more studies would be required.

Timeliness is also another factor that impacts the results. On the one side, as the digital life on social networks evolves very fast: if the data we used were not recent, our analysis might produce results no longer meaningful. To mitigate this risk, we used a data leak from less than 5 years ago, and even so a few identities were obsolete.

5. Conclusions and future work

This study introduces different methods and techniques that an attacker could use to get and combine data about digital identities and how these data could be exploited by using a System of Systems perspective. The records from a Digital Pluridentity Persona can be modeled with the Digital Persona Portrayal Metamodel described in this study. Two sub-models have been designed that ease the matching among the gathered data and the security: DPKM and RSM. These models can be used to systematically analyze the security of the systems regarding the DP through a Digital Pluridentity Persona Portrayal Analysis. This supports a tangible study of the exposition in any system on which the identities of the DP could be used. In this way, the security is evaluated based on how a DP becomes vulnerable by combining the information the individual systems are providing, from a SoS perspective.

The presented model and method have been used in a study to assess the security of 17 chosen anonymized candidates. The DP3A method helped in organizing the data gathered from the individual to analyze and detect vulnerabilities that could impact on the security on the DP of the individuals. This overexposure could be used to execute social engineering attacks and exploit the systems whose security is knowledge-based.

Our method can be used either in blind way, simulating a real attacker that can only use the information they can find, or for self-analysis, by leveraging own complete knowledge and matching the information across different identities.

Although our study revealed how pluridentities put us at risk, on the other hand Internet users are becoming more and more aware about the relevance of privacy and about the potential impact of publishing their personal data on the Internet. Thus, to conclude with a positive remark, we can say that the more conscious people becomes, the harder it will become to find evidences of insecurities in the digital life by using this method.

This study is part of the ongoing work TeSSoS [39], which describes five stages for assessing the security in the SoS context. TeSSoS begins with *SoS Discovery* stage to define the scope of the SoS. Then, vulnerabilities are revealed during the *Red Requirements* stage, and the countermeasures for the vulnerabilities are defined in the *Blue Requirements* one. Security Implementation focuses on development and training. Finally, the countermeasures are evaluated and validated by trying to exploit the previously defined vulnerabilities.

The two first stages of TeSSoS are implemented in this study: Digital Persona Portrayal implementing the *SoS Discovery* and Digital Persona Security Analysis as *Red Requirements*. The three remaining stages of validation are considered as Future work, as well as implementing TeSSoS in other SoS architectures.

Additionally, three validation works are scheduled. The first one is based in applying expert judgment methods to the modeling, security, and testing-related issues by using Delphi method [10].

Then, an industrial validation of this approach is intended to be performed in collaboration with some companies by studying the exposure of their employees by using this approach and evaluate if the overexposure could become a vulnerability not only for the employees but also for the organization as a SoS on which employees are considered as constituent systems. In this way the security team of the company can establish some metrics on how exposed the employees are and adjust the privileges of each individual or design defensive strategies.

A third validation is considered to realize about the feasibility of evolve a system by developing some vulnerabilities' countermeasures defined as Blue Requirements in those constituents' systems that allow it.

This kind of validations have been conducted previously by coauthors with satisfactory results as in [14,49,50].

The described future work includes testing this method by simulating real attacks. For instance, companies can use this approach to evaluate the level of exposure of their employees. However, some considerations shall be pointed out because the validation may be threatened due to ethical considerations. On one hand, the potential attacks need to be permitted by the candidates before to be launched, on the other hand, the candidates shall not be informed in advance of the attack, because this can affect their reactions if an interaction happens, producing inaccurate results [5,28].

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Miguel Angel Olivero: Conceptualization, Methodology, Software, Writing - original draft, Writing - review & editing, Data curation. **Antonia Bertolino:** Writing - original draft, Writing - review & editing, Conceptualization. **Francisco José Domínguez-Mayo:** Visualization, Investigation, Writing - original draft, Writing - review & editing, Conceptualization. **María José Escalona:** Supervision, Investigation. **Ilaria Matteucci:** Supervision, Writing - original draft, Writing - review & editing.

Acknowledgments

This study has been partially supported by the GAUSS National Research project (MIUR, PRIN 2015, Contract 2015KWREMX) and by the Spanish Ministry of Economy and Competitiveness (POLOLAS, TIN 2016-76956-C3-2-R). We would also like to thank the *Privacy Service Research Area CNR in Pisa* for their support and the anonymous reviewers for their comments that greatly contributed to improve this study.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2020.102492.

References

[1] Abass IAM. Social engineering threat and defense: a literature survey. J Inf Secur 2018;9(4):257–64.

[2] Aktypi A, Nurse JRC, Goldsmith M. Unwinding Ariadne's identity thread: privacy risks with fitness trackers and online social networks. In: MPS 2017 - Proceedings of the 2017 workshop on multimedia privacy and security, co-located with ccs 2017; 2017.

[3] Antonius N, Rich L. Discovering collection and analysis techniques for social media to improve public safety. Int Technol Manage Rev 2013.

[4] Atote BS, Zahoor S, Dangra B, Bedekar M. Personalization in user profiling: privacy and security issues. In: Int. conf. on internet of things and applications IOTA, Pune; 2016. p. 415–17.

[5] Carpenter S, Zhu F, Kolimi S. Reducing online identity disclosure using warnings. Appl Ergon 2014.

[6] Clarke R. The digital persona and its application to data surveillance. Inf Soc 1994;10(2):77–92. online at http://www.rogerclarke.com/DV/DigPersona.html#DP accessed January 2020.

[7] Clarke R., http://www.rogerclarke.com/ID/IdModel-Gloss-1002.html, 2010. (accessed January 2020).

[8] Creese S, Goldsmith M, Nurse JRC, Phillips E. A data-reachability model for elucidating privacy and security risks related to the use of online social networks. In: Proc. of the 11th ieee int. conference on trust, security and privacy in computing and communications, trustcom-2012 - 11th Ieee int. conference on ubiquitous computing and communications, IUCC-2012; 2012.

[9] Dahmann JS, Baldwin KJ. Understanding the current state of US defense systems of systems and the implications for systems engineering. In: IEEE Int syst conf proceedings, SysCon; 2008. p. 99–105.

[10] Dalkey N, Helmer O. An experimental application of the Delphi method to the use of experts. Manage Sci 1963;9(3):458–67. doi:10.1287/2Fmnsc.9.3.458.

[11] Di Martino M, Robyns P, Weyts W, Quax P, Lamotte W, Andries K. Personal information leakage by abusing the GDPR 'Right of access'. Fifteenth symposium on usable privacy and security; 2019.

[12] El-Maliki T, Seigneur JM. User-centric mobile identity management services. In: Int conf emerg secur information, syst technol; 2007. p. 33–76.

[13] Emanuel L, Bevan C, Hodges D. What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces. Conference on human factors in computing systems - proceedings; 2013.

[14] Escalona MJ, López G, Vegas S, et al. A software engineering experiments to value MDE in testing. Learning lessons XXI JISBD; 2016.

[15] European Union. General data protection regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 2016. (accessed January 2020).

[16] Foozy C, Ahmad R, Abdollah M. Generic taxonomy of social engineering attack. In: Malaysian tech univ int conf eng technol MUiCET; 2011. p. 527–33. MUiCET.

[17] Garfinkel SL. Email-based identification and authentication: an alternative to PKI? IEEE Secur Privacy 2003.

[18] Gross R, Acquisti A, Heinz HJ. Information revelation and privacy in online social networks. WPES'05: proceedings of the 2005 acm workshop on privacy in the electronic society; 2005.

[19] Gupta P, Gottipati S, Jiang J, Gao D. Your love is public now: questioning the use of personal information in authentication. In: ASIA ccs 2013 - Proceedings of the 8th acm sigsac symposium on information, computer and communications security; 2013.

[20] HaveIBeenPwned. https://haveibeenpwned.com/ (accessed January 2020).

[21] How to get started in online investigations with open-source intelligence. Medium. https://medium.com/1st-draft/how-to-get-started-in-online-investigations-with-open-source-intelligence-71d0ddc0f639.

[22] Hodges D, Creese S, Goldsmith M. A model for identity in the cyber and natural universes. In: Proceedings - 2012 European intelligence and security informatics conference; 2012.

[23] Hutchings A., Pastrana S. Understanding eWhoring. 2019. arXiv:1905.04576.

[24] Identity Leak Checker. Hasso-Plattner-Institut https://sec.hpi.de/ilc/.

[25] ISO/IEC is 21839:2019: systems and software engineering — system of systems (SoS) considerations in life cycle stages of a system. International Organization for Standardization, Geneva, Switzerland.

[26] Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Commun ACM 2007;50(10):94–100.

[27] Jamshidi M. System of systems engineering: Innovations for the 21st century. Wiley series in systems engineering and management. Hoboken, NJ: John Wiley & Sons, Inc; 2009.

[28] Krasnova H, Günther O, Spiekermann S, Koroleva K. Privacy concerns and identity in online social networks. Identity Inf Soc 2009.

[29] Maier MW. Architecting principles for systems-of-systems. Syst Eng 1998.

[30] Malhotra A, Totti L, Meira W, Kumaraguru P, Almeida V. Studying user footprints in different online social networks. In: Proceedings of the 2012 ieee/acm international conference on advances in social networks analysis and mining, asonam 2012; 2012.

[31] Mansour RF. Understanding how big data leads to social networking vulnerability. Comput Human Behav 2016;57:348–51.

[32] My data request. https://mydatarequest.com/ (accessed January 2020).

[33] Minkus T, Ding Y, Dey R, Ross KW. The city privacy attack: combining social media and public records for detailed profiles of adults and children. In: COSN 2015 - Proceedings of the 2015 ACM conference on online social networks; 2015.

[34] Mitnick KD, Simon WL. The art of deception: controlling the human element of security. W. Publishing., Ed. Indianapolis: Wiley Publishing; 2002.

[35] Mouton F, Malan MM, Leenen L, Venter HS. Social engineering attack framework. In: Inf secur south Africa - Proc ISSA; 2014. p. 1–9. Conf.

[36] Mueller ML, Park Y, Lee J, Kim TY. Digital identity: how users value the attributes of online identifiers. Inf Econ Policy 2006;18(4):405–22.

[37] Nurse JRC, Erola A, Gibson-Robinson T, Goldsmith M, Creese S. Analytics for characterising and measuring the naturalness of online personae. Secur Inf 2016.

[38] Olivero MA, Bertolino A, Dominguez-Mayo FJ, Escalona MJ, Matteucci I. Addressing security properties in systems of systems: challenges and ideas. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics); 2019.

[39] Olivero MA, Bertolino A, Dominguez-Mayo FJ, Escalona MJ, Matteucci I. Security assessment of systems of systems. SESoS 2019.

[40] OMG, OMG unified modeling language, v2.5. http://www.omg.org/spec/UML/, 2015 (accessed January 2020).

[41] Perito D, Castelluccia C, Kaafar MA, Manils P. How unique and traceable are usernames?. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics); 2011.

[42] Qiu L, Lu J, Yang S, Qu W, Zhu T. What does your selfie say about you? Comput Human Behav 2015.

[43] Rabkin A. Personal knowledge questions for fallback authentication: security questions in the era of facebook. In: SOUPS 2008 - Proceedings of the 4th symposium on usable privacy and security; 2008.

[44] Reese K, Smith T, Dutson J, Armknecht J, Cameron J, Seamons K. A usability study of five two-factor authentication methods. In: Proc. the 15th symposium on usable privacy and security (SOUPS); 2019.

[45] Salahdine F, Kaabouch N. Social engineering attacks: a survey. Fut Internet 2019;11(4):89.

[46] Shirey, R.W. Internet security glossary, version 2. https://tools.ietf.org/pdf/rfc4949.pdf 2007 (accessed January 2020).

[47] Spiderfoot. https://www.spiderfoot.net/documentation/#what-is-spiderfoot/ 2019 (accessed January 2020).

[48] Tajbakhsh M, Homayounvala E, Shokouhyar S. Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage. Int J Electron Secur Digit Forensics 2017;9(1):62.

[49] Torrecilla CJ, Escalona MJ, Mejías M. A Delphi-based expert judgment method applied to the validation of a mature Agile framework for web development projects. IT&M 2018:1–32. doi:10.1007/s10799-018-0290-7.

[50] Urbieta M, Escalona MJ, Rossi G, Robles-Luna E. Detecting conflicts and inconsistencies. web application requirements. Lect Notes Comput Sci 2012;1(7959):278–88. doi:10.1007/978-3-642-27997-3_27.

[51] Wayman JL. Biometrics in identity management systems. IEEE Secur Privacy 2008;6(2):30–7.

[52] Zheqiang-Gong N, Liu B. You are who you know and how you behave: attribute inference attacks via users' social friends and behaviors. In: SEC16 – Proceedings of the 25th usenix conference on security symposium; 2016.